IMPROVISASI ALGORITMA RSA MENGGUNAKAN GENERATE KEY ESRKGS PADA INSTANT MESSAGING BERBASIS SOCKET TCP

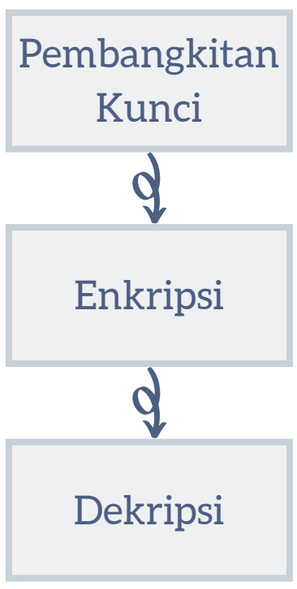
GADHING PUTRA ADITYA
201510370311061

ABSTRAK

Socket TCP adalah abstraksi yang digunakan aplikasi untuk mengirim dan menerima data melalui koneksi antar dua host dalam jaringan komputer. Jaringan yang biasa kita gunakan bersifat publik yang sangat rentan akan penyadapan data. Masalah ini dapat teratasi dengan menggunakan algoritma kriptografi, salah satunya menggunakan algoritma RSA. Tingkat keamanan algoritma RSA standar memiliki celah keamanan pada kunci publik ataupun privat yang berasal dari inputan 2 bilangan prima saat pembangkitan kunci, begitupun dengan algoritma improvisasi RSA meskipun menggunakan 4 buah bilangan prima. Peningkatan keamanan dapat dilakukan dengan memodifikasi algoritma RSA dengan menggunakan ESRKGS (Enhanced and Secured RSA Key Generation Scheme). ESRKGS RSA memiliki kelebihan yang utama pada segi keamanannya. ESRKGS RSA secara total memodifikasi algoritma RSA terutama pada bagian pembangkitan kunci. Hasil pengujian performa waktu pembangkitan kunci dengan panjang bit 256 bit, 512 bit, dan 1024 bit serta untuk proses enkripsi dan dekripsi panjang karakter yang digunakan adalah 100, 250, dan 400 menunjukkan bahwa algoritma ESRKGS RSA lebih baik dibandingkan algoritma improvisasi RSA. Pengujian kemanan menggunakan known plaintext attack dan fermat factorization attack menunjukkan bahwa algoritma ESRKGS RSA lebih baik dibandingkan algoritma RSA standar dan improvisasi RSA.

METODE PENELITIAN

1. RSA Standar
2. Improvisasi RSA
3. ESRKGS RSA



PENGUJIAN

1. Algoritma Terhadap Aplikasi

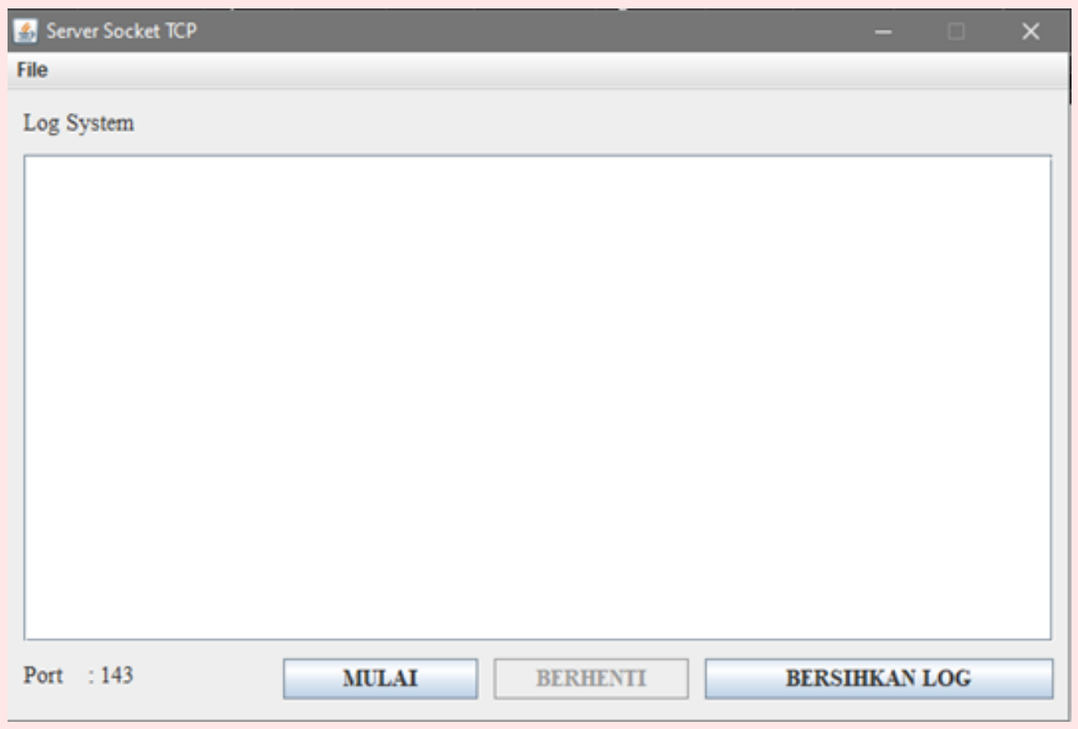
- Perhitungan Manual
- Perhitungan Sistem

2. Performa

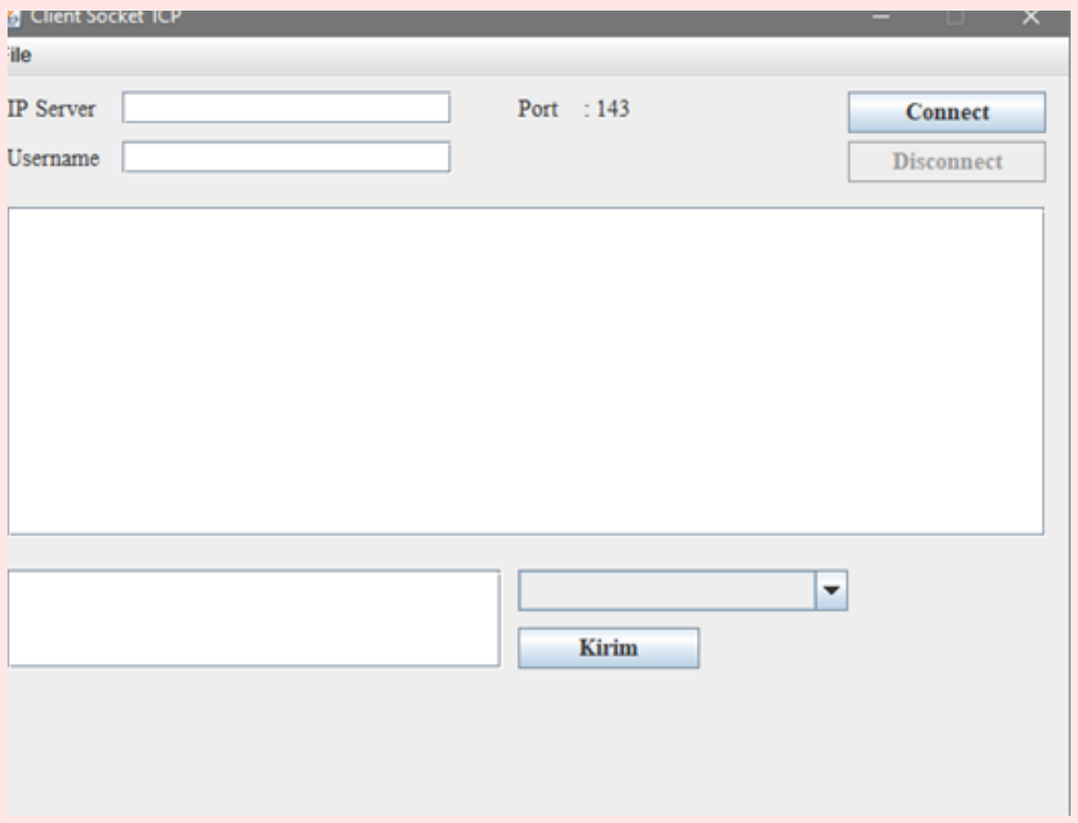
- Performa Pembangkitan Kunci
- Performa Enkripsi
- Performa Dekripsi

3. Keamanan

- Known Plaintext Attack
- Fermat Factorization Attack



Tampilan Server Socket TCP



Tampilan Client Socket TCP

KESIMPULAN

Penelitian yang sudah dilakukan dapat ditarik beberapa kesimpulan diantaranya adalah algoritma RSA standar, improvisasi RSA, dan ESRKGS RSA dapat diimplementasikan pada aplikasi instant messaging socket TCP, algoritma ESRKGS RSA memiliki performa yang lebih baik dari improvisasi RSA akan tetapi masih dibawah dari RSA standar dikarenakan beberapa factor yang mempengaruhi pada saat proses pembangkitan kunci, enkripsi, dan dekripsi, serta algoritma ESRKGS RSA memiliki tingkat keamanan yang lebih baik dibandingkan RSA standar dan improvisasi RSA, dibuktikan dengan tidak ditemukannya kunci privat pada dua metode pengujian serangan yaitu known plaintext attack dan fermat factorization attack.